EUROPEAN COMMISSION
European Education, and Culture Executive Agency

RECORD OF PERSONAL DATA PROCESSING

Art. 31 REGULATION (EU) 2018/1725 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (henceforth the "Regulation")

Record nº | *N° 2022-15*

In accordance with Article 31 of Regulation 2018/1725, individuals whose personal data are processed by the Agency in any context whatsoever are to be protected with regard to the processing of personal data and the Agency has to keep records of their processing operations.

This record covers two aspects:
1. Mandatory records under Art 31 of the Regulation (recommendation: make the header and part 1 publicly available)
2. Compliance check and risk screening (initial; part 2 is internal only to the Agency, not published)

The ground for the record is (tick the relevant one):

☒ *Regularization of a data processing operation already carried out*
☒ *Record of a new data processing operation prior to its implementation*
☐ *Change of a data processing operation*
☐ *Migration from notification to record.*

Internal control activities in EACEA	
1	**Last update of this record (where applicable)**
	This is an updated version of ARES(2022)8220635 to include all IC activities
2	**Short description of the processing**
	Assessment of the internal control systems of EACEA through the performance of ad hoc analysis/survey aimed at different goals, as follow up of deviations and any detected internal control weakness or calculation of indicators.
Part 1 - Article 31 Record	
3	**Name of the Controller** **Unit(s) and/or function of person acting on behalf of the Controller**

	Controller: European Education, and Culture Executive Agency Unit(s): the person designated as being in charge of the processing operation is the Head of Unit of EACEA.R2.002 (Budget and Control) Email: EACEA-INTERNAL-CONTROL@ec.europa.eu
4	**Contact details of the Data Protection Officer (DPO)**
	EACEA-data-protection@ec.europa.eu
5	**Name and contact details of joint controller (where applicable)**
	NA
6	**Name and contact details of processor (where applicable)**
	NA
7	**Purpose of the processing**
	EACEA internal control team continuously assesses the effectiveness of its internal control system (ongoing monitoring) and performs a comprehensive analysis (separate assessment) at least once a year. The ad hoc analysis, calculation of indicators and internal control survey described in this data record allow for both the control activities. The analysis cannot be performed if access to personal data is not granted. This particularly refers to, but not exclusively, access to data of Human Resources nature. The Internal Control Manager receives mostly lists including also EACEA staff information. The purpose is not to gather personal data but, by default, in these lists personal data is included. Also, according to EACEA's internal control framework (Communication to the Commission from Commissioner Oettinger: Revision of the internal control framework C(2017) 2373 dated 19 April 2017) final related to Internal Control Principle 16, EACEA should assess the effectiveness of its internal control system at least once a year. As part of this assessment, a survey to staff and to managers is carried out on an annual basis regarding selected internal control issues. There are two sets of questions, one for staff and one for management. The survey is anonymous, and no link will be made between the answers given and the identity of the participants. The staff participating to the survey is selected from a list provided by Unit R1, including all EACEA staff. The methodology and participation is prepared by EACEA's sector responsible for internal control issues and decided by the EACEA's RMIC. EACEA uses the survey results and comments made to analyse the effectiveness of its internal control system. As a follow-up of the control activity the survey's outcome will be used to publish a report and to set up an action plan with implementing measures, if deemed necessary. The survey is carried out with the support of EU Survey IT tool from DIGIT.
8	**Description of the categories of data subjects**
	☒ Agency staff (Contractual and temporary staff in active position) ☐ Visitors to the Agency ☒ Contractors providing goods or services ☐ Applicants

	☐ Relatives of the data subject ☐ Complainants, correspondents and enquirers ☐ Witnesses ☒ Beneficiaries ☐ External experts ☐ Contractors ☐ Other, please specify:
9	**Description of personal data categories**
	Indicate <u>all</u> the categories of personal data processed and specify which personal data are being processed for each category (between brackets under/next to each category): ***a) Categories of personal data:*** ☐ in the form of personal identification numbers ☐ concerning the physical characteristics of persons as well as the image, voice or fingerprints ☐ concerning the data subject's private sphere ☐ concerning pay, allowances and bank accounts ☐ concerning recruitment and contracts ☐ concerning the data subject's family ☐ concerning the data subject's career ☐ concerning leave and absences ☐ concerning missions and journeys ☐ concerning social security and pensions ☐ concerning expenses and medical benefits ☐ concerning telephone numbers and communications ☒ concerning names and addresses (including email addresses) ☒ Other: please specify: **grade and unit (for EACEA staff)** ***b) Categories of personal data processing likely to present <u>specific risks:</u>*** ☐ data relating to suspected offences, offences, criminal convictions or security measures ☐ data being used to evaluate personal aspects of the data subject (ability, efficiency, conduct) ***c) Categories of personal data whose processing is <u>prohibited</u>, with exceptions (art. 10):*** ☐ revealing racial or ethnic origin ☐ revealing political opinions ☐ revealing religious or philosophical beliefs ☐ revealing trade-union membership ☐ concerning health ☐ genetic data, biometric data for the purpose of uniquely identifying a natural person

	☐ concerning sex life or sexual orientation ***d) Specify any additional data or explanatory information on the data being processed, if any:*** NA
10	**Retention time (time limit for keeping the personal data)**
	For the purpose of the current process, EACEA.R2.002 applies the principles and retention periods indicated in Common Retention List of the Commission, by analogy[1]. Files covering the definition, adoption, application and coordination of the implementation of internal controls are kept for 7 years. After that period, they are erased. **Indicate the period of storage:** 7 years from the reception of the data **Is any further processing for historical, statistical or scientific purposes envisaged?** ☐ yes ☒ no **If yes, indicate the further retention time:** NA
11	**Recipients of the data**
	Personal data are kept in restricted folders, access is given on a need-to know basis to the following recipients: • EACEA Director • EACEA Internal Control Manager and Staff members from Sector R2.002 (Performance, Audit and Internal Control) • EACEA R2 unit management • Staff in the European Commission DG DIGIT as managing EU Survey IT tool. In addition, in case of control or dispute, personal data can be shared with and processed by the bodies charged with a monitoring or inspection task in application of Union law in compliance with the applicable data protection rules and within the scope of their tasks entrusted by the relevant legislation. This includes, in particular, the following recipients: - The European Court of Justice or a national judge as well as the lawyers and the agents of the parties in case of a legal procedure; - The European Anti-Fraud Office (OLAF); - The Internal Audit Service of the Commission - The Investigation and Disciplinary Office of the Commission (IDOC) - The European Court of Auditors - The European Ombudsman - The European Public Prosecutor's Office - EU courts and national authorities
12	**Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?**
	NO
13	**<u>General</u> description of the technical and organisational security measures**
	Access to data is only possible on a need-to-know basis and for the set purposes. Data is kept confidential and stored in restricted folders.

[1] SEC(2022)400 category 12.11

	The European Commission's IT systems used by the Agency abide by the Commission's security guidelines. The Agency must comply with Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission. 1. Organisational measures: A Corporate Local Informatics Security Officer (C-LISO) is in place. Its role includes supervising the Agency compliance with the relevant regulations, and the application of security measures recommend by DIGIT. Organisational measures include appropriate access rights and access control. As a rule within the Agency, access to information systems, the file system or offices are subject to a series of authorisations where the person granting the access is different from the person requesting or authorising the access - except in limited cases of delegation. The responsible person in the unit in charge of this action (processing operation of the current record) collects and places the documents on the secured drives of the Commission and all Agency staff are bound by a confidentiality obligation. The need to know principle applies in all cases. 2. Technical measures: State of the art technical cybersecurity measures are implemented in the corporate systems, according to the security needs. Those measures are in constant evolution.
14	**Information to data subjects / Data Protection Notice (DPN)**
	Two data protection Notices are published in the EACEA internal control intranet page, one is general and the other one is dedicated to the survey and also linked to the survey itself, in order to make it easily accessible to respondents.

Qualified electronic signature by:
MARCO CARNACCINI
Date: 2024-07-29 17:52:47 +02:00